Novel Knowledge Graph-Based Modeling for Vulnerability Detection in the Internet of Medical Things

Kulsoom Saima Bughio[1][0000−0003−4046−9578], David Cook[1][0000−0002−2264−8719], and Syed Afaq Ali Shah[1][0000−0003−2181−8445]

Edith Cowan University, 270 Joondalup Dr, WA, 6027, Australia[1]

Abstract. In the evolving landscape of the Internet of Medical Things (IoMT) cybersecurity, traditional security measures often struggle with complex vulnerabilities, which are crucial due to the sensitive nature of patients' data. This article addresses this challenge and presents a semantic framework to enhance cybersecurity on IoMT. It proposes a novel MIoT (Medical Internet of Things) ontology that integrates knowledge from diverse sources and employs RDF (Resource Description Framework) formalism for the semantic representation of medical devices and their related aspects. The framework also utilizes semantic modelling to enrich data annotation and knowledge base development, supporting the detection of vulnerabilities in medical IoT (Internet of Things) networks. Additionally, the framework generates a knowledge graph that stores Cyberthreat Intelligence (CTI) for medical IoT networks, enhancing vulnerability detection, while underscoring the significance of automated reasoning over aggregated knowledge.

Keywords: Internet of Medical Things (IoMT)· MIoT (Medical Internet of Things) Ontology· Vulnerability Detection· Knowledge Graph · Cyberthreat Intelligence· Automated Reasoning

1 Introduction

Smart technologies have reshaped how humans engage with their environment, offering unprecedented convenience, efficiency, and automation. From smart homes and cities to the expansive Internet of Things (IoT), these innovations aim to intelligently integrate digital and physical systems. Artificial intelligence (AI) serves as a pioneering force in this technological evolution, profoundly impacting daily life. Its integration into the IoT has transformed interactions, enhancing service quality, efficiency, and overall productivity [1].

The Internet of Medical Things (IoMT) is a specific subset of IoT that is particularly transformative. It refers to the interconnected system of medical devices, software applications, health systems, and services that communicate with each other and with healthcare IT systems. The IoMT encompasses wearable devices such as fitness trackers, implanted devices such as heart monitors, and even hospital-based systems like surgical robots. The primary goal is to

optimize patient care, enhance the quality and effectiveness of treatments, and increase the overall efficiency of healthcare delivery [2].

Since IoMT devices often deal with sensitive personal health information, they are potential targets for cyberattacks. The security concerns include data breaches, unauthorized access, and the potential for cybercriminals to manipulate medical devices, which could lead to life-threatening outcomes. For instance, in 2022, the U.S. Department of Health and Human Services reported 125 digital data breaches in healthcare nearly doubling from the previous year [3]. The upward trend persisted into early 2023, with 145 reported incidents in healthcare in the first quarter [4]. In March 2023, a report from HIPAA (The Health Insurance Portability and Accountability Act) highlighted a concerning pattern, with data breaches affecting over 4 million patients [5].

However, the integration of IoMT into healthcare systems brings forth significant security concerns. The rapid alteration in IoT applications in healthcare makes it challenging for cyber threats and vulnerabilities in knowledge organization systems. Very few systems can work in IoMT to model it in terms of interoperability and heterogeneity. In the case of medical devices, when any cyber-attack (i.e. ransomware or phishing) has occurred, the organization systems are not well developed to provide semantic knowledge to improve cyber resilience. This paper provides the basis for developing the knowledge graph-based modeling for vulnerability detection in the IoMT setting, that is ultimately exploit attacks.

The rest of the paper is organised as follows. Section 2 discusses 'Related Work', followed by Section 3, which presents our Proposed Framework for Vulnerability Detection Utilizing Knowledge Graph-Based Modeling. Section IV provides a discussion. The conclusion and future work are presented in Section V.

2 Related Work

Several researchers work in IoMT settings and have proposed systems to enhance the security and privacy of patients by using different techniques such as ensemble learning, federated learning, blockchain machine learning and deep learning methods. Alsubaei et al. [6] proposed a Python-based recommendation tool utilizing an MIoT ontology, tailored to stakeholder-specific needs and scenario-based approaches. The tool's effectiveness was assessed through a vulnerability-based method and an expert-based method, involving the evaluation of 40 vulnerabilities from the NVD (National Vulnerability Dataset) dataset across 11 scenarios and incorporating recommendations from seven cybersecurity graduates. Their tool faces a few challenges, particularly in the complexity of IoMT environments, ensuring adaptability to evolving IoMT solutions, and the potential difficulty for certain stakeholders, such as medical professionals and patients, to comprehend its recommendations. Additionally, it requires regular updates to address new IoMT solutions and security threats.

Recently, Khan et al., [7] proposed a Secure Ensemble Learning-Based Fog-Cloud Approach for Cyberattack Detection in IoMT, which addresses the se-

curity issues in IoMT networks caused by cyberattacks. One of the limitations of this research is that their approach was evaluated using a simulated environment, which may not accurately reflect the real-world performance of their approach. Additionally, the proposed approach may not be effective against new and unknown cyberattacks that have not been included in the training dataset. The research presented by [8] focuses on Federated Learning (FL), Artificial Intelligence (AI), and Explainable AI (XAI) in the context of intelligent healthcare. The primary aim is to address vulnerabilities and challenges in traditional healthcare systems that rely on centralized data sharing. In terms of challenges they faced, these include privacy issues, difficulties in aggregating user data from different sources, the potential failure of cloud systems in personalized settings, and the sensitivity of healthcare data.

The survey paper proposed by Jameel Almalki [9] focuses on analyzing current state-of-the-art blockchain technologies and their applications in IoT-based healthcare systems. It acknowledges the diversity in both the dimensions of existing blockchain approaches and the requirements of IoT-based healthcare applications. The main limitations identified include unresolved security issues such as hostile attacks and authentication challenges, ongoing issues with blockchain delay, and a lack of in-depth performance evaluation of the system. In another survey [10], researchers focus on exploring the use of modern technologies like the Internet of Things (IoT), 5G networks, artificial intelligence (AI), and big data analytics in enhancing healthcare solutions. It emphasizes the need for continued research to enhance the security aspects of modern healthcare systems, thereby addressing the prominent open-ended research challenges identified in the survey. Mahmood et al. [11] conducted a Systematic Literature Review focused on developing a security model for the IoMT. This involved analyzing major security models and conducting a meta-analysis to prioritize risks. The resulting model includes a Python-based interface for identifying and managing threats. However, the article recognizes the necessity for ongoing enhancements to the model, acknowledging the dynamic nature of security threats in the IoMT sector.

Sills et al., [12] aim to address security vulnerabilities in medical IoT devices by creating a comprehensive repository of Cyber Threat Intelligence (CTI), enabling the use of AI-based cyber defence systems. For this purpose, they proposed a system that generates CTI from sources such as manufacturer alerts, and ICS-CERT[1], and augments it with data from Wikidata and FDA[2]'s AccessGUDID. The combined information forms a Cybersecurity Knowledge Graph (CKG) that is further enhanced through graph embeddings. However, the lack of extensible big data resources for medical device vulnerabilities necessitates the need for knowledge augmentation, and the complexity of connecting diverse data sources in the CKG is one of the challenging tasks. Secondly, security risks associated with medical IoT devices, such as data breaches and device compromise, high-

[1] Industrial Control Systems - Cyber Emergency Response Team
[2] Food and Drug Administration

light the urgency of creating a reliable knowledge base to enhance cybersecurity measures in healthcare settings.

Apart from this, the literature focused on the key research areas in the field of IoMT to address security and privacy concerns [13], [14], [15]. Additionally, there's a growing focus on developing regulatory frameworks and standards [16], [17] to ensure IoMT devices meet minimum security requirements [18], [19]. However, they lack to provide semantic information for medical devices in terms of vulnerability detection. In contrast to existing techniques, this paper proposes a semantic framework to facilitate partial automation in improving the security posture of medical devices in remote patient monitoring (RPM). At the heart of this framework will be a domain ontology, which captures the semantics of the concepts and properties of the main security aspects of IoT devices used in such systems. This will be complemented by a security ruleset, complex queries, and a mechanism to enable automated reasoning over the aggregated knowledge.

3 A Proposed Framework for Vulnerability Detection Utilizing Knowledge Graph-Based Modeling

In this section, we present our proposed framework for vulnerability detection. This framework integrates the Internet of Medical Things ontology, a knowledge graph enriched with medical device data, and the incorporation of the National Vulnerability Database (NVD) CVE information via an API[3]. This methodology empowers the framework to offer predictions about vulnerabilities, thereby enhancing the security of remote patient monitoring systems. Figure 1 shows the working mechanism of our proposed approach. The details of each component including data storage and processing are provided in the following sections.

3.1 Knowledge Acquisition

The knowledge acquisition phase involves gathering comprehensive background knowledge from different sources such as literature, existing ontologies, standards, vocabularies, and manufacturers. This background knowledge is related to the fields of cybersecurity and IoMT, particularly remote patient monitoring. This process includes identifying commonly used medical devices in the IoMT settings, understanding potential vulnerabilities and attacks targeting these devices, and determining the relevant security requirements. Standards and vocabularies such as RDFs (Resource Description Frameworks) and schema.org are utilized to identify and represent the necessary data for developing the domain ontology IoMT. Data related to different types of IoT devices used in remote patient monitoring, potential cyberattacks, and their corresponding data types and functionality is collected. Extensive literature surveys are conducted to review existing ontologies in the cybersecurity field, such as the VulOntolog [19], which provides valuable concepts and properties that can be incorporated into

[3] Application Programming Interface

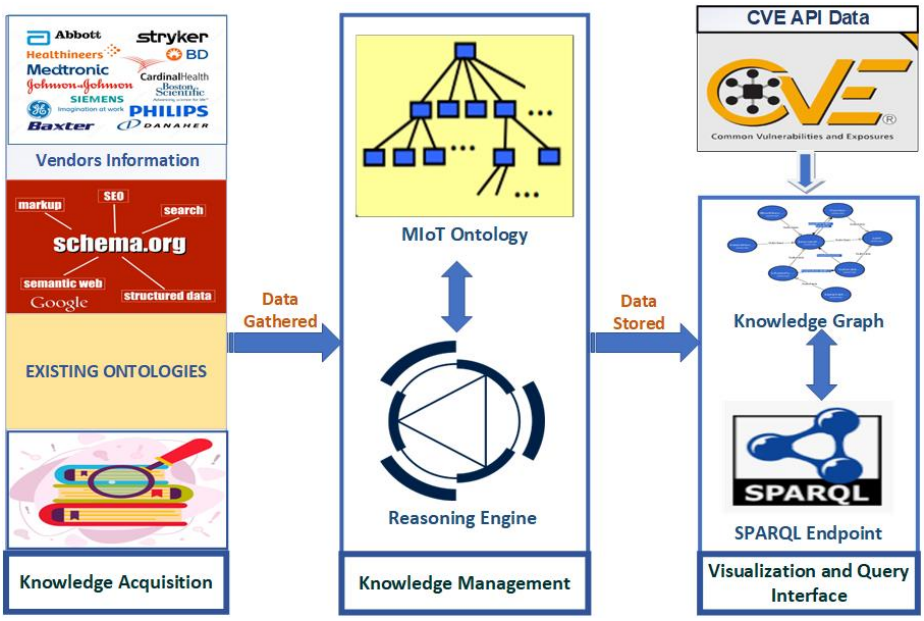

Fig. 1. A Semantic Framework for Vulnerability Detection based on Knowledge Graph (Source of Images: Google).

the IoMT ontology for effective cybersecurity in remote patient monitoring systems.

3.2 Knowledge Management

Knowledge management plays a crucial role in our proposed framework, utilizing reasoning to infer new facts within the ontology. The framework employs rule-based reasoning, wherein rules are defined to describe logical conditions and to predict hidden relationships within the ontology. Knowledge management can be divided into two main parts, as follows:

MIoT Ontology The development of an MIoT ontology for cybersecurity in remote patient monitoring systems starts with data acquisition, followed by defining relevant concepts and properties and annotating the data with semantic information. The MIoT ontology is central, incorporating healthcare expertise and literature to define the semantics of medical devices, vulnerabilities, and services. It uses RDF formalism for better representation and supports vulnerability detection in Medical IoT by enhancing data access, sharing, and automated reasoning. This ontology includes various concepts such as medical devices, vulnerabilities, users, etc., and their relationships, contributing significantly to IoMT security. The key purpose of MIoT ontology is:

Data Annotation: This involves annotating data with semantic information using the MIoT ontology to enhance the semantics of the RPM domain. The ontology encompasses concepts related to vendors, products, medical devices, manufacturers, firmware, versions, vulnerabilities, exploits, and affected components of medical devices, including OS, hardware, and applications.

Knowledge Base Development: This process utilizes concepts, instances, and their relationships derived from knowledge acquisition. The knowledge base comprises a collection of data points (instances) and the categories or ideas they represent (concepts), all interconnected through relationships. This structure is vital for organizing and interpreting complex, diverse information in a meaningful way, particularly in domains like IoMT.

Reasoning Engine Extending the domain ontology with rules and complex queries enables reasoning capabilities that go beyond simple data retrieval. It can identify potential vulnerabilities, assess the impact of vulnerabilities, and recommend mitigation strategies based on the knowledge encoded within the ontology and the rules.

For instance, this framework may employ a rule that associates a particular firmware version with a known vulnerability based on the NVD dataset. "This rule allows us to identify all devices with the same firmware, version as potentially vulnerable". By utilizing complex queries, we can further analyse the network topology, device configurations, and other relevant factors to assess the potential impact of these vulnerabilities on the overall system.

Our framework facilitates automated reasoning over aggregated data from various sources, such as the MIoT ontology, CVE information, and any other external source. In rule-based reasoning, rules are used as a fundamental mechanism to draw conclusions or make decisions. Rule-based systems evaluate data or facts against these rules to infer new information or make decisions.

For example:

X= CardiacRhythmManagement is a MedicalSensor

Y= MedicalSensor is a subClassOf MedicalIoTDevice

Z= CardiacRhythmManagement is a MedicalIoTDevice

In the rule-based systems, this transitive property shows If X=Y and Y=Z then X=Z.

In rule-based reasoning, software agents efficiently apply predefined rules to data, identifying relevant patterns and executing corresponding actions or conclusions. Their automated processing capabilities are essential for decision-making or in environments where human expertise needs to be emulated or augmented. For example, a rule state that:

"If a medical device firmware version x from the vendor y is known to have a specific vulnerability (based on historical data or NVD CVE information), then all devices with the same firmware version are considered vulnerable". This rule is represented in SWRL (Semantic web Rule Language) and DL (Description Logic) syntax as follows:

SWRL Rule

Product(?product) $\wedge$ *hasFirmware(?product, ?firmware)* $\wedge$ *hasVendor (?product, ?vendor)* $\wedge$ *hasVulnerability(?firmware, true)* $\wedge$ *Product (?otherProduct)* $\wedge$ *hasFirmware(?otherProduct, ?firmware)* $\wedge$ *hasVendor (?otherProduct, ?vendor)* $\wedge$ *DifferentFrom(?product, ?otherProduct)* $\rightarrow$ *is vulnerable(?product, true)*

DL Axioms

$\forall x.\, Product(x) \wedge \exists f.\, hasFirmware(x, f) \wedge \exists v.\, hasVendor(x, v)$
$\wedge \exists w.\, hasVulnerability(f, w) \wedge w = true \rightarrow isVulnerable(x, true)$

This axiom shows that, if a product has firmware with a vulnerability, then the product is vulnerable.

$\forall x. \forall y. \forall f. \forall v.\, Product(x) \wedge Product(y) \wedge hasFirmware(x, f) \wedge hasFirmware(y, f)$
$\wedge hasVendor(x, v) \wedge hasVendor(y, v) \wedge x \neq y \rightarrow isVulnerable(x, true)$
$\wedge isVulnerable(y, true)$

This axiom shows that, if two different products have the same firmware and the same vendor, then both products are vulnerable.

3.3 Visualization and Query Interface

The ontology data is stored in a knowledge graph, which also includes the data source NVD (National Vulnerability Database) with its Common Vulnerabilities and Exposures (CVE) data to display vulnerabilities associated with medical devices in the ontology. The knowledge graph provides visualization capabilities, allowing users to view the relationships and connections within the graph. Additionally, it offers a SPARQL endpoint that enables users to query the graph and assess the effectiveness of the framework. It consists of three parts:

MIoT Knowledge Graph A knowledge graph is a graph-based data structure that represents knowledge through entities, relationships, and attributes. It offers a flexible way to organize, query, and enhance understanding of data. In this framework, a knowledge graph is proposed, based on the developed MIoT ontology. The initial version of MIoT ontology is published in [21]. Utilizing semantic modelling and the NVD dataset, this cybersecurity knowledge graph is populated with Cyber Threat Intelligence (CTI) about vulnerabilities in medical devices within IoT networks.

In this research, we are using the OntoText GraphDB [4] tool to generate the MIoT knowledge Graph that stores the CTI of IoT networks in medical devices.

[4] https://www.ontotext.com/

This facilitates the detection of vulnerabilities, thereby strengthening the protection of patient data. Figure 2 illustrates the domain-range graph for the MIoT knowledge graph. Where it showcases the various concepts (i.e., Vulnerability, Vendor, Services etc.,) and their relationships (i.e., hasVendor, byUsingService, usingDevice etc.,) with the concept Product.

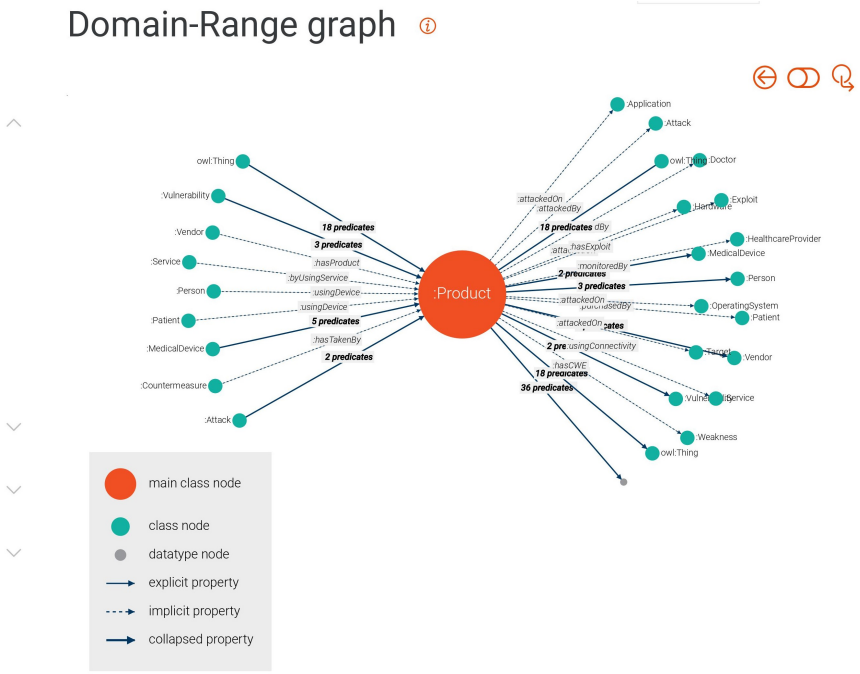

Fig. 2. The Domain-Range graph for the concept *Product*.

Integration with Industry Standards The National Vulnerability Database (NVD) is a U.S. government repository that provides standards-based vulnerability management data. This includes details on security-related software flaws, misconfigurations, product names, and impact metrics. The NVD is essential for the IT security community, offering a comprehensive database to evaluate and manage cybersecurity risks linked to known vulnerabilities in software products and systems. It serves as a crucial tool for cybersecurity professionals to identify and address vulnerabilities in network and software environments.

In our framework, we utilize the NVD dataset for a detailed analysis of vulnerabilities in medical IoT networks. The NVD offers a standardized collection of known vulnerabilities and exploits in such settings. Our integration of this dataset allows us to identify specific vulnerabilities in these systems. We seam-

lessly incorporate the NVD by utilizing an API to access up-to-date information on CVE and the Common Vulnerability Scoring System (CVSS). The NVD API allows users to access NVD data and allows the integration of this information into our framework programmatically. The API can be used to automatically update security systems with the latest vulnerability information, including security checklists, security-related software flaws, product names, and impact metrics. This ensures that our framework is continuously updated with the latest data from the NVD, providing ongoing protection against new threats in remote patient monitoring IoT networks.

Access the SPARQL Endpoint The SPARQL endpoint enables access to the knowledge graph's interface, allowing users, including patients, doctors, and healthcare providers, to visualize, query, and update data. For example:

```
SELECT ?Product ?Condition ?y ?p ?e
WHERE {
    ?Product a base:MedicalSensor .
    ?Product MIoT:monitor ?Condition .
    ?x base:vulnerabilityID ?y.
    ?x base:hasPublished ?p.
    ?x base:hasExploit ?e.
    filter (?y = "CVE-2023-1729") .
}
```

The above-mentioned query retrieves all those products whose CVE ID is CVE-2023-1729, along with other relevant information such as functionality provided by the product, its published date, and exploit.

```
SELECT ?Product ?Condition ?y ?p ?w
WHERE {
    ?Product a base:MedicalSensor .
    ?Product MIoT:monitor ?Condition .
    ?x base:vulnerabilityID ?y.
    ?x base:hasPublished ?p.
}
```

This query retrieves those products with the name of medicalSensor along with their functionality, VulnerabilityID and when it was published.

4 Discussion

In the rapidly evolving domains of IoT and cybersecurity for IoMT, existing security measures often fall short, especially in handling complex vulnerabilities with significant semantic implications. These shortcomings are critical due to the sensitive nature of patient data, underscoring the need for improved, automated

security solutions on the Internet of Medical Things (IoMT). Several ontologies addressing various aspects of this domain have been published in the realm of IoT and Medical Things (IoMT) and cybersecurity to [6], [20], [22], [23] among others. However, our proposed research introduces a comprehensive ontology that represents medical devices, users, vendors, vulnerabilities, and more within the RPM cybersecurity context. This ontology aims to capture the domain's semantics and establish meaningful relationships between entities.

Additionally, a significant deficiency of traditional security measures is their lack of automation. This issue becomes particularly problematic in the rapidly changing cybersecurity landscape, where new vulnerabilities constantly emerge. Without automated systems to quickly identify and respond to these threats, there's a delay between the emergence of a vulnerability and its mitigation. This delay allows attackers to exploit these weaknesses before users or administrators become aware of them. This situation underscores the need for more dynamic, intelligent, and automated security solutions in the IoMT field, capable of proactively addressing threats in real-time to protect sensitive patient data. Existing knowledge graphs populate NVD CVE information from JSON/XML4[5] files of the NVD dataset. Our framework stands out by using an API to access and incorporate data, ensuring regular updates and the ability to address emerging vulnerabilities.

5 Conclusion and Future Work

In this research article, we propose a semantic framework that combines the Medical Internet of Things (MIoT) ontology with a knowledge graph enriched by medical device data and integrates CVE information from the National Vulnerability Database (NVD) via an API. Our approach enables the system to detect vulnerabilities, thereby improving the security of remote patient monitoring systems. The knowledge graph concisely presents Cyber Threat Intelligence (CTI) information, offering advantages over traditional relational databases. In addition, we demonstrate the importance of automated reasoning over aggregated knowledge by presenting example rules. Future work will focus on employing a reasoning engine to perform automated reasoning, aimed at identifying vulnerabilities. This will allow the framework to generate advanced alerts about vulnerabilities and potential attacks.

Disclosure of Interests. The authors declare no conflict of interest.

References

1. Banaeian Far S., Imani Rad A.: Internet of Artificial Intelligence (IoAI): the emergence of an autonomous, generative, and fully human-disconnected community. Discover Applied Sciences, **6,3**, pp. 6:91. (2024). https://doi.org/10.1007/s42452-024-05726-3.

[5] JavaScript Object Notation/Extensible Markup Language

2. Niu, Q., Li, H., Liu, Y., Qin, Z., Zhang, L., Chen, J., Zhihan, L.: Toward the Internet of Medical Things: Architecture, trends and challenges. Mathematical Biosciences and Engineering **21** pp. 650–678, (2023).
3. Doyle P.,: Healthcare breaches on the rise in 2022. Accessed on 25-12-2023. https://www.techtarget.com/searchsecurity/news/252521771/Healthcare-breaches-on-the-rise, (2023).
4. Doug B.: Top healthcare data breach statistics of 2023. Persona. (2023).
5. Journal, H.: More Than 4 Million Individuals Affected by Cyberattack on Independent Living Systems. THE HIPAA JOURNAL. (2023).
6. Alsubaei, F., Abuhussein, A., Shiva, S.: Ontology-Based Security Recommendation for the Internet of Medical Things. IEEE Access **7**, pp. 48948–48960 (2019). https://doi.org/10.1109/ACCESS.2019.2910087.
7. Khan, F., Jan, M. A., Alturki, R., Alshehri, M. D., Shah, S. T., Rehman, A. U.: A Secure Ensemble Learning-Based Fog-Cloud Approach for Cyberattack Detection in IoMT. IEEE Trans Industr Inform **19, 10**, pp. 10125–10132. (2023). https://doi.org/ 10.1109/TII.2022.3231424.
8. Kulshrestha, P., Kumar TV. Vijay.: Machine learning based intrusion detection system for IoMT. International Journal of System Assurance Engineering and Management (2023). https://doi.org/10.1007/s13198-023-02119-4.
9. Almalki, J.: State-of-the-Art Research in Blockchain of Things for HealthCare. Arab J Sci Eng, (2023). https://doi.org/10.1007/s13369-023-07896-5.
10. Jagatheesaperumal, S.K., Mishra, P., Moustafa, N., Chauhan, R.: A holistic survey on the use of emerging technologies to provision secure healthcare solutions. Computers and Electrical Engineering **99** (2022) 107691. https://doi.org/10.1016/j.compeleceng.2022.107691.
11. Mahmood, M. et al.: Improving Security Architecture of Internet of Medical Things: A Systematic Literature Review. IEEE Access **11**, pp. 107725–107753, (2023). https://doi.org/10.1109/ACCESS.2023.3281655.
12. Sills, M., Ranade, P., Mittal, S.: Cybersecurity Threat Intelligence Augmentation and Embedding Improvement - A Healthcare Usecase. Proceedings - 2020 IEEE International Conference on Intelligence and Security Informatics, ISI 2020, (2020). https://doi.org/ 10.1109/ISI49825.2020.9280482.
13. Rahman A. et al.: Federated learning-based AI approaches in smart healthcare: concepts, taxonomies, challenges and open issues. Springer US **26, 4**, (2023). https://doi.org/10.1007/s10586-022-03658-4.
14. Awotunde, J.B., Chakraborty, C., Folorunso, S. O.: A Secured Smart Healthcare Monitoring Systems Using Blockchain Technology. Internet of Things, pp. 127–143, (2022). https://doi.org/10.1007/978-3-030-81473-1_6.
15. Otoum, Y., Wan, Y., Nayak, A.: Federated Transfer Learning-Based IDS for the Internet of Medical Things (IoMT). 2021 IEEE Globecom Workshops, GC Wkshps 2021 Proceedings, pp. 1–6. (2021). https://doi.org/10.1109/GCWkshps52748.2021.9682118.
16. Frey, B. B.: Health Insurance Portability and Accountability Act. The SAGE Encyclopedia of Educational Research, Measurement, and Evaluation **1996**, pp. 12–14, (2018). https://doi.org/10.4135/9781506326139.n302.
17. Therapeutic Goods Administration: Medical device cyber security guidance for industry. pp. 1–55.(2021).
18. Nasiri, S., Sadoughi, F., Tadayon, M. H., Dehnad, A.: Security requirements of internet of things-based healthcare system: A survey study. Acta Informatica Medica **27, 4**, pp. 253–258. (2019). https://doi.org/10.5455/aim.2019.27.253-258.

19. Yaqoob, T., Abbas, H., Atiquzzaman, M.: Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices-A Review. IEEE Communications Surveys and Tutorials, **21, 4**, pp. 3723–3768. (2019). https://doi.org/10.1109/COMST.2019.2914094.
20. Qin, S., Chow, K.P.: Automatic Analysis and Reasoning Based on Vulnerability Knowledge Graph. Springer Singapore, (2019). https://doi.org/10.1007/978-981-15-1922-2.
21. Bughio, K. S.: Knowledge Organization System for Partial Automation to Improve the Security Posture of IoMT Networks. Procedia Comput Sci, **225**, pp. 3471–3478, (2023). https://doi.org/10.1016/j.procs.2023.10.342.
22. Christian, R., Dutta, S., Park, Y., Rastogi,N.: An Ontology-driven Knowledge Graph for Android Malware. Proceedings of the ACM Conference on Computer and Communications Security, pp. 2435–2437, (2021). https://doi.org/10.1145/3460120.3485353.
23. Sharma, N. et al.: A smart ontology-based IoT framework for remote patient monitoring. Biomed Signal Process Control, **vol. 68**, p. 102717, (2021). https://doi.org/10.1016/j.bspc.2021.102717.